CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

1-6. (Cancelled)

7. (Currently amended) A restricted data format method for a network infrastructure copy protection system, comprising:

receiving a digital content file for transmission across a distributed computer network;

examining data comprising the content file to determine whether the content file includes a restricted data format, the examining performed within the distributed computer network~~, and wherein the restricted data format including at least one of a MP3 data format, a MPEG video data format, and a Word document format~~;

transmitting the content file when data comprising the content file does not include the restricted data format; and

blocking transmission of the content file when data comprising the content file does include the restricted data format to prevent unauthorized downloading of copyrighted material, wherein the blocking is effected prior to a transmission of the content file to a receiver.

8-10. (Cancelled)

11. (Original) The method of Claim 7 wherein the distributed computer network is the Internet.

12. (Original) The method of Claim 7 wherein the examining is performed by a plurality of routers within the distributed computer network.

13. (Original) The method of Claim 7 wherein the examining is performed by a plurality of cache engines within the distributed computer network.

14-16. (Cancelled)

17. (Currently amended) A ~~network infrastructure protection~~ method ~~for detecting and denying transmission of restricted data formats,~~ comprising:

receiving a digital content file for transmission across a distributed computer network;

~~using at least one router configured to log digital signatures related to the digital content file to maintain a record for the digital content file and the related digital signatures, the record including the related digital signatures,~~ examining ~~data comprising~~ the digital content file to determine whether the digital content file comprises one or more signatures, wherein the one or more signatures identify one or more senders that requested transmission of the digital content file across the distributed computer network ~~a restricted data format, wherein the digital content file is free of a digital signature, the examining performed within the distributed computer network, and wherein the restricted data format including at least one of a MP3 data format, a MPEG video data format, and a Word document format~~; and

logging the digital content file and the one or more signatures in a log, wherein the log of the one or more signatures is maintained to determine an identity of the one or more senders of the digital content file.

~~transmitting the digital content file when the data comprising the digital content file does not include the restricted data format; and~~

~~blocking the transmission of the digital content file when the data comprising the digital content file does include the restricted data format to prevent unauthorized downloading of copyrighted material, wherein the blocking is effected prior to a transmission of the digital content file to a receiver~~.

18-20. (Cancelled)

21. (Currently amended) A network device comprising:

a bus;

computer readable memory units connected to said bus;

one or more processors coupled to said bus said computer readable memory units for executing a digital signature method for a network infrastructure copy protection system, comprising:

~~applying a digital signature to a digital content file;~~

examining ~~the~~ a digital content file to determine whether the digital content file includes ~~the~~ a digital signature, wherein the examining is performed within the distributed computer network;

logging the digital content file and the digital signature to create a file transmission log;

transmitting the digital content file when the digital content file includes the digital signature; and

blocking transmission of the digital content file when the digital content file does not include the digital signature to prevent unauthorized downloading of copyrighted material, wherein the blocking is effected prior to a transmission of the digital content file to a receiver; and

identifying a sender of the digital content file according to the digital signature included in the file transmission log after the digital content file has been transmitted.

~~blocking transmission of the digital content file when the data comprising the content files is a restricted data format to prevent unauthorized downloading of copyrighted material, wherein the restricted data format including at least one of a MP3 data format, a MPEG video data format, and a Word document format.~~

22. (Currently amended) The device of Claim 21 wherein the file transmission log is configured to maintain a plurality of digital signatures associated with a single ~~digital signature is configured to identify the sender of the~~ digital content file, where each of the plurality of digital signatures is logged for a separate transmission of the digital content file.

23. (Previously presented) The device of Claim 21 wherein the digital signature applied to the content file within the distributed computer network is logged to maintain a record for the content file and the digital signature when the content file is transmitted across the distributed computer network.

24. (Previously presented) The device of Claim 21 wherein the distributed computer network is the Internet.

25. (Previously presented) The device of Claim 21 wherein the examining is performed by a plurality of routers within the distributed computer network.

26. (Previously presented) The device of Claim 21 wherein the examining is performed by a plurality of cache engines within the distributed computer network.

27. (Currently amended) A ~~network device comprising:~~

~~one or more network interfaces;~~

~~computer readable memory units connected to said one or more network interfaces;~~

~~one or more processors coupled to said bus said computer readable memory units for executing a method for detecting and denying transmission of restricted data formats,~~ method comprising:

receiving a digital content file ~~for transmission across a distributed computer network~~;

examining the digital content file for inclusion of a first digital signature;

logging the digital content file and the first digital signature;

verifying an authenticity of the first digital signature, wherein the first digital signature is associated with a first user;

transmitting the digital content file including the first digital signature;

receiving the digital content file;

examining the digital content file for inclusion of a second digital signature;

logging the digital content file and the second digital signature;

verifying an authenticity of the second digital signature, wherein the second digital signature is associated with a second user; and

transmitting the digital content file including the second digital signature ~~using at least one router configured to log digital signatures related to the digital content file to maintain a record for the digital content file and the related digital signatures, the record including the~~

~~related digital signatures, examining data comprising the digital content file to determine whether the digital content file comprises a restricted data format, wherein the digital content file is free of a digital signature, the examining performed within the distributed computer network, and wherein the restricted data format including at least one of a MP3 data format, a MPEG video data format, and a Word document format;~~

~~transmitting the digital content file when the data comprising the digital content does not include the restricted data format; and~~

~~blocking the transmission of the digital content file when the data comprising the digital content file does include the restricted data format to prevent unauthorized downloading of copyrighted material, wherein the blocking is effected prior to a transmission of the digital content file to a receiver~~.

28-29. (Cancelled)

30. (Currently amended) A ~~restricted data format~~ system ~~for a network infrastructure copy protection system,~~ comprising:

means for receiving a ~~digital content~~ file ~~for transmission across a distributed computer network~~;

means for examining ~~data comprising~~ the ~~content~~ file to determine whether the ~~content~~ file includes one or more signatures ~~a restricted data format~~, the examining performed within the distributed computer network~~, and wherein the restricted data format including at least one of a MP3 data format, a MPEG video data format, and a Word document format~~;

means for transmitting the ~~content~~ file across a distributed computer network when ~~data comprising~~ the content file does not include the one or more signatures ~~restricted data format; and~~

means for blocking transmission of the ~~content~~ file when ~~data comprising~~ the ~~content~~ file does include the one or more signatures ~~restricted data format to prevent unauthorized downloading of copyrighted material~~, wherein the blocking is effected prior to a transmission of the ~~content~~ file to a receiver; and

means for maintaining a log of the file and the one or more corresponding signatures, wherein the log is maintained to identify one or more senders of the file after the file has been transmitted across the distributed computer network.

31. (Currently amended) A ~~network infrastructure protection~~ system ~~for detecting and denying transmission of restricted data formats,~~ comprising:

means for receiving a digital content file for transmission across a distributed computer network;

means for using at least one router configured to log one or more digital signatures related to the digital content file to maintain a record for the digital content file and the related digital signatures, the record including the related digital signatures[[,]];

means for examining data comprising the digital content file to ~~determine whether the digital content file comprises~~ identify the one or more digital signatures ~~a restricted data format, wherein the digital content file is free of a digital signature, the examining performed within the distributed computer network, and wherein the restricted data format including at least one of a MP3 data format, a MPEG video data format, and a Word document format~~;

means for transmitting the digital content file when the data comprising the digital content file does not include the one or more digital signatures ~~restricted data format~~; and

means for blocking the transmission of the digital content file when the data comprising the digital content file does include the one or more digital signatures; and ~~restricted data format to prevent unauthorized downloading of copyrighted material, wherein the blocking is effected prior to the transmission of the digital content file to a receiver~~

means for analyzing the record to identify one or more senders associated with the one or more digital signatures, wherein the record is configured to maintain a plurality of digital signatures for a digital content file that is transmitted by a plurality of senders.

32. (New) The method of Claim 31 further comprising:

means for identifying a plurality of senders that transmitted the digital content file across the distributed network, each of the plurality of senders associated with one or more of the plurality of digital signatures.

33. (New) The method of Claim 7 further comprising:

examining data associated with the digital content file to identify one or more digital signatures associated with one or more senders of the digital content file;

maintaining a log of each transmission of the digital content file and the associated one or more digital signature; and

identifying the one or more senders from the log after the transmission of the digital content file.

34. (New) The method of Claim 17 wherein the log is capable of maintaining a plurality of signatures associated with a single digital content file.

35. (New) The method of Claim 34 further comprising:

identifying a plurality of senders associated with the plurality of signatures, wherein one or more of the plurality of signatures is logged each time the digital content file is transmitted across the distributed computer network.

36. (New) The method of Claim 27 wherein a log is maintained of the digital content file and both of the corresponding first and second digital signatures.

37. (New) The method of Claim 36 further comprising:

identifying the first and second users from the first and second digital signatures maintained in the log.

38. (New)The system of Claim 30 wherein the log is configured to maintain a plurality of digital signatures for a single file that is transmitted multiple times across the distributed network.